

Remarks

It is to be noted that this application has been previously examined and a substantive report issued. This application is a National Stage of a PCT application designating the United States, which application is treated as a US patent application. During the International Preliminary Examination Phase an Examiner at the British Patent Office issued an International Preliminary Examination Report which was attached to the papers submitted to the USPTO and therefore the Examiner certainly has a copy of it.

In paragraph 1 of the official action the Examiner sets forth a number of matters, including what appears to be objections to claims 1, 12, 15 and 22. With respect to claim 1, the Examiner seems to assert that the terms "...the trusted device...a true value of an integrity metric..." require "clarification, precision or correction".

The Examiner's objection is not understood. The phrase "trusted device" is used at several points of the present application. Please see, for example, the discussion beginning at page 3, line 26 and continuing on through page 4, line 34. See also the discussion beginning at page 5, line 32 and continuing through page 7, line 24. With respect to the true value of an integrity metric, the Examiner's attention is directed to the discussion at, for example, page 7, line 33 through page 9, line 25.

With respect to the term "a challenge" in claim 12, the Examiner is referred to the disclosure at page 11, lines 13-24.

With respect to claim 15, the Examiner finds the language "...to verify the integrity metric and the nonce..." apparently to be unclear. With respect to this terminology, the Examiner is referred to page 11, lines 17-32 of the specification.

It is submitted that the language used in the claims is consistent with the language used in the specification and that the use in the claims meets the clarity requirements of 35 U.S.C. 112, second paragraph. With all due respect to the Examiner, our patent statute gives the Applicant the privilege of providing claims directed to the "subject matter

which the Applicant regards as his invention." See 35 U.S.C. 112, second paragraph. Doubtlessly, the Examiner would claim this invention differently, but the statutory language gives the Applicant the privilege of deciding how the invention should be claimed. If the Examiner still believes that the claims are unclear, the Examiner is invited to specify, with particularity, exactly why he believes the claims to be unclear.

The present title of this application is "Trusted Computing Platform". The Examiner asserts that this title is not descriptive. With all due respect to the Examiner, the title is descriptive, and certainly differentiates this invention from the prior art cited by the Examiner, which will be discussed subsequently.

Under a subtitle "oaths" the Examiner states that the "missing signatures of Graeme John Proudler, Dipankar Gupta, Liqun Chen and Siani Lynne Pearson will be required in the next response." It is assumed that the Examiner is trying to assert that the inventors' declarations filed in this application lack the signatures of the persons identified above. However, that is not the case. Enclosed herewith is a copy of a paper filed on December 5, 2001 explaining the copies of the various declarations which were filed and the persons who signed them. The very persons which the Examiner identifies in the official action have previously signed declarations, so the Examiner's comment about "missing signatures" is in error. In addition to enclosing a copy of the December 5, 2001 paper, we also enclose a copy of the postcard by which the USPTO acknowledged receipt of all of those documents and copies of the enclosures to the December 5, 2001 paper.

In the International Preliminary Examination Report the British Examiner took the position that claims 1-11 were either anticipated or obvious over EP 0849657 and that claims 12-21 patentably defined over that art.

In the instant official action, the Examiner does not reference the prior examination of this application, but rather seemingly starts matters anew. However, since the US Examiner has not repeated the citation of that art, it is assumed that the Examiner of the opinion that the action by the British Examiner was inappropriate and/or that the

citation has been withdrawn.

Claim 1 was amended when the national stage was entered in order to address the British Examiner's comments regarding the clarity of claim 1 found in section VIII of the International Preliminary Examination Report.

In the official action, the Examiner cites US Patent No. 6,473,800 and rejects the claims based upon that document. Those rejections will now be discussed.

In part two of the official action, the Examiner rejects claims 1-10, 12-17 and 22-43 under 35 U.S.C. 102 as allegedly being fully anticipated by US Patent No. 6,473,800 to Jerger et al. This grounds for rejection is respectfully traversed.

Claim 1 recites a computing apparatus comprising "main processing means" and "main memory means" which are "mounted on an assembly" and "being connected for communication with one or more other components on the assembly". The invention of claim 1 further comprises a "trusted device mounted on the assembly and being connected for communications with one or more other components on the assembly, the trusted device being arranged to acquire a true value of an integrity metric of the computing apparatus" as is recited in claim 1.

It is not understood what Jerger has to do with the foregoing. Jerger is directed to downloading of active content through a browser and the issue of what permissions may be given to such content. See Jerger page 2, line 27 through page 3, line 3. Jerger does not seem to be at all concerned with the trustworthiness of the platform to which the active content is to be downloaded. It is apparently assumed that the platform is trustworthy and under the user's control. It should be noted that the Jerger patent is assigned to Microsoft Corporation and, indeed, as the Examiner is no doubt well aware, the Microsoft Windows operating system has been criticized for lack of trustworthiness controls. It is believed that, to a person skilled in the art, there is nothing in the Jerger disclosure which a person of ordinary skill in the art would characterize as being a "trusted device" in terms of acquiring "an integrity metric of the computing system" as

claimed.

The Examiner points to Figure 1 as depicting a "trusted device". Just where in Figure 1 is such a device shown? The rules of practice require that the Examiner point out, with specificity, just how he is reading the claims on the cited reference. 37 CFR 1.104(c)(2) specifically requires that when a reference is "complex or shows and describes inventions other than that claimed by the Applicant, the particular part relied upon must be designated as nearly as practicable." Is Figure 1 of the Jerger patent as close as the Examiner can get to designating exactly which component or components read upon the recitation of the "trusted device" of claim 1?

With all due respect to the Examiner, it is submitted that a person skilled in the art would not refer to that which is shown in Figure 1 and call any of it a "trusted device" given the fact that it is well known in the art that the device of Figure 1 is easily violated.

Given the fact that the Examiner has not identified just which device or element shown in Figure 1 is the "trusted device" of claim 1, only tempts the Applicant to speculate as to just why claim 1 is being rejected. The rules of practice, quoted above, make it clear that the Applicant does not have to speculate as to why his claims are being rejected, but rather the onus is on the Examiner to set forth his rejections clearly. That the Examiner has not done and therefore, with all due respect to the Examiner, the Examiner is respectfully requested to follow the rules of practice.

Turning to Figure 1 of the Jerger patent, just which element or elements shown thereon meet the "main memory means" and "trusted device" limitations set forth in claim 1? Claim 1 also recites that the trusted device is "arranged to acquire a true value of an integrity metric of the computing apparatus." Note the fact that the integrity metric is with respect to the computing apparatus. This is completely consistent with the description at pages 7 and 8 of the application as filed. Note that in one embodiment the integrity metric is acquired by a measurement function which generates a digest of the BIOS (Basic Input/Output Software) instructions in the BIOS memory. See column 7,

lines 26-28 and claims 23 and 24 (which are not dependent upon claim 1, but rather dependent upon claim 22) and new claims 45 and 46.

Figure 1 of the Jerger patent certainly shows a BIOS 126. If claims 23 and 24 are really fully anticipated by Jerger, then where is there any disclosure in Jerger of (i) "an integrity metric of the computing apparatus" as specifically recited in claim 1, (ii) "an integrity metric that measures that the computing apparatus is operating as intended" as recited in claim 22, (iii) an integrity metric which is "a digest of all or part of the Basic Input/Output Software for the computing apparatus" as specifically recited by claim 23 or (iv) an integrity metric which is "a digest of all or part of the Basic Input/Output Software for the components or apparatus attached to the computing apparatus" as specifically recited in claim 24?

The Examiner refers the Applicant to column 6, lines 8-41 where the Examiner asserts that "the true code value of integrity is exacted, compared and verified by the computing apparatus of Figure 1". Assuming for the moment that the Examiner's assertion is correct, how does that have anything to do with the language of the claims? The Jerger patent appears to be concerned with a security model for managing active content downloaded from a computer network. What does that have to do with the present invention which is concerned with the integrity of the computing apparatus itself? If the computing apparatus itself has been compromised, then worrying whether or not there is rogue code in the active content downloaded from a computer network is a bit like worrying about whether or not the barn door has been closed after the horses have escaped.

In view of the fact that the Examiner has not identified "an integrity metric of the computing apparatus" in the Jerger patent and since it is axiomatic that the Examiner must show where each and every limitation of claim 1 (and the other rejected claims) can be found in the Jerger patent in order to sustain a rejection under 35 U.S.C. 102, the rejection must fail.

Turning to claim 12, which the Examiner rejects as allegedly being fully anticipated by

the Jerger patent, where is there any disclosure of “the trusted device acquiring the true value of the integrity metric of the computing apparatus”? The Examiner points to Figure 1, but simply pointing to Figure 1 does not comply with the rules of practice as previously noted and the Examiner is respectfully requested to comply with the rules of practice should the Examiner continue to cite the Jerger patent or any other prior art document against any of the claims in this application.

Claim 12 also recites “the user generating a challenge for the trusted computing apparatus to prove its integrity...” Where is that shown or suggested by Jerger? The Examiner points the Applicant to column 5, line 52 through column 6, line 7 where the Examiner asserts that a challenge is performed. Assuming that the Examiner’s assertion is correct, how does any such challenge relate to proving the integrity of the trusted computing apparatus as set forth in the second step of claim 12?

The Applicant believes that Jerger is utterly irrelevant to the claims in this application and therefore the Examiner is respectfully requested to reconsider the rejection of those claims.

New claims 44-52 are added by this response. All of the added claims are dependent claims and it is submitted that the claims from which they depend clearly define over Jerger. As such, there is no need to discuss the inventive nature of the subclaims presently pending in this application. It is also believed that if the Examiner reads pages 7-9 of the application as filed he will find adequate support for the newly added dependent claims. For example, the first whole paragraph on page 7 of the application as filed discusses the possibility that the trusted device may be implemented as either an application specific integrated circuit in one embodiment or as an appropriately programmed microcontroller in another embodiment. Claims 47 and 48 are directed to those two separate possible embodiments.

With respect to new claim 52 which recites “means for testing to assure that the trusted device is accessed by said main processor before said main processor accesses Basic Input/Output Instructions for booting the computing apparatus”. The Examiner’s

attention is directed to the disclosure on page 8 of the application at lines 9-25.

Reconsideration is respectfully requested.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 12-0415. In particular, if this response is not timely filed, then the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136 (a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 12-0415.

I hereby certify that this correspondence is being deposited with the United States Post Office with sufficient postage as first class mail in an envelope addressed to Commissioner for Patents

POB 1450, Alexandria, VA 22313-1450 on

November 10, 2003

(Date of Deposit)

Richard P. Berg


(Name of Person Signing)

(Signature)

November 10, 2003

(Date)

Respectfully submitted,



Richard P. Berg
Attorney for Applicants
Reg. No.28,145
LADAS & PARRY
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300

Enclosures:

-5 Replacement Drawings Sheets
-copy of filing dated December 5, 2001
including date stamped postcard listing the
attachments